



UNITED STATES PATENT AND TRADEMARK OFFICE

5a
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/963,789	09/27/2001	Keisuke Takemori	011152	9137
38834	7590	04/26/2005	EXAMINER	
WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP 1250 CONNECTICUT AVENUE, NW SUITE 700 WASHINGTON, DC 20036			PYZOCZA, MICHAEL J	
		ART UNIT		PAPER NUMBER
				2137

DATE MAILED: 04/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/963,789	TAKEMORI ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 27 September 2001.
 2a) This action is FINAL. 2b) This action is non-final.
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-20 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) Claim(s) _____ is/are allowed.
 6) Claim(s) 1-20 is/are rejected.
 7) Claim(s) _____ is/are objected to.
 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
 10) The drawing(s) filed on 27 September 2001 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>01292002, 11122004</u> . | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____ |

Art Unit: 2137

DETAILED ACTION

1. Claims 1-20 are pending.

Claim Objections

2. Claim 1 is objected to because of the following informalities: "access to the" in line 7 would read more clearly as "access from the". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1, 10-11, 14-20 are rejected under 35 U.S.C. 102(a) as being anticipated by ITL Bulletin (hereinafter ITL).

As per claim 1, ITL discloses an intrusion preventing system which prevents an intrusion to regular data storage means connected to a network, comprising: decoy data storage means which is provided separately from the regular data storage means; and guiding means which guides an illegal access to the

Art Unit: 2137

regular data storage means into the decoy data storage means (see page 4 column 3).

As per claim 10, ITL discloses the regular data storage means is a regular server, and the decoy data storage means is a decoy server provided together with the regular server (see page 4 column 3).

As per claim 11, ITL discloses intrusion judging means which judges whether or not a communication session established between the regular server and an external terminal is due to intrusion; communication session relaying means which relays a communication session which has been judged as an intrusion from the regular server to the decoy server; and path switching means which transfers a packet whose destination is the regular sever to the decoy server in a communication session which has been judged as the intrusion (see page 4 column 3 and page 2 column 3 which discloses a packet-based IDS).

As per claims 14-15, IT discloses a buffer for transfer which sequentially stores the same packets as packets whose destinations are the regular server; and a buffer for return which sequentially returns responses returned from the decoy server, wherein, when the communication session which has been judged as the intrusion is relayed to the decoy server, the buffer for transfer sequentially outputs the responses from the

Art Unit: 2137

first packet which has been returned in response to the first packet transferred after relayed (see page 4).

As per claim 16, ITL discloses pseudo response means which, without transferring a packet whose destination has been converted from the regular server to the decoy server, creates a response command to the packet in a pseudo manner to return the same (see page 4).

As per claim 17, ITL discloses when a source address of a communication session, which has been judged as intrusion is stored and a packet containing the source address is then input, a communication session is established between the decoy server and the user (see page 4).

As per claim 18, ITL discloses in the communication session established between the decoy server and the user, action logs and trace data of the user are collected (see page 4).

As per claim 19, ITL discloses the path switching means includes means which converts the content of the response command returned from the decoy server to the content of a response command which will be output when the regular server receives a packet (see page 4 where this is inherent because if this step did not occur the user would know it has been switched to a different server).

Art Unit: 2137

As per claim 20, ITL discloses an intrusion preventing system which prevents an intrusion to a regular region of a server connected to a network, wherein without allowing access to the regular region for an access command whose destination is the regular region, a pseudo response command expressing a message where the access to the regular region has been succeeded is returned response to the access to the regular region (see page 4 column 3).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 2-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over ITL as applied to claim 1 above, and further in view of Golan (US 5974549).

As per claim 2, ITL fails to disclose the decoy and regular data storage means are on the same server, with the decoy means being secured.

Art Unit: 2137

However, Golan teaches such regions on the same system (see column 2 lines 13-28).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Golan's method of secure regions in the IDS system of ITL.

Motivation to do so would have been to only allow certain APIs to execute (see Golan column 2 lines 39-48).

As per claim 3, the modified ITL and Golan system discloses destination rewriting means, which rewrites a destination of an access, which is the server to the decoy region (see ITL page 4).

As per claim 4, the modified ITL and Golan system discloses response rewriting means which rewrites the content of a response command returned in response to an access to the decoy region to the content of a response command which is to be returned in response to an access to the regular region (see ITL page 4).

As per claims 5-7, the modified ITL and Golan system discloses monitors whether or not an access whose destination is the regular region is an illegal access, wherein the destination rewriting means rewrites the destination of an illegal access to the decoy region (see ITL page 4).

Art Unit: 2137

As per claim 8, the modified ITL and Golan system discloses the regular region and the decoy region are allocated with a common IP address (see page 4 as applied to the cited Golan sections).

As per claim 9, the modified ITL and Golan system discloses means that collects action logs or trace data of a session guided to the decoy region (see ITL page 4).

7. Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over ITL as applied to claim 10 above, and further in view of FOLDOC.

As per claims 12-13, ITL fails to disclose the response from the decoy server would be the same (or mirrored) as the regular server.

However, FOLDOC teaches mirroring (see page 1).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use mirroring from FOLDOC with the IDS of ITL.

Motivation to do so would have been to protect the data (see FOLDOC page 1).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Bace (An

Art Unit: 2137

Introduction to Intrusion Detection and Assessment) discloses the use of a decoy server to which hackers are redirected, Network Associates (Next Generation Intrusion Detection in High-Speed Networks) discloses sacrificial servers with dummy data, Huff et al (US 6408391) discloses intrusion detection with redirection do dummy data, Moran (US 6826697) discloses honey pots with trap hosts, and Sorkin et al (US 20020157021) discloses honey pots with trap hosts.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2137

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJP

**ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER**